Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Emerging Trends and Innovations in Electronics and Communication Engineering - ETIECE-2017

Volume 5, Special Issue 01, Jan.-2018 (UGC Approved)

Analysis of LSB and DWT Steganography Techniques over Various Attacks

Syed Mujtiba Hussain[1], Salihah Yousu[1], Syed Bisma[1], Mehvish Siddiqi[1], ZahidGulzar Khaki[2]

[1]*Department of Computer Science and Engineering, Islamic University of Science and Technology.*
[2]*Department of Electronics and Communication Engineering, Islamic University of Science and Technology.*

ABSTRACT: *Due to phenomenal increase in the concern about security and confidentiality of information over the internet, various techniques have been proposed. Steganography is one such technique. It's a form of security from obscurity. a Steganography is a technique of hiding one piece of information into another. In this paper we make comparisons between two steganography techniques one from spatial domain (LSB) and other from frequency domain (DWT) on the basis of various attacks. No doubt LSB provides high PSNR and good image quality but it's not so robust to attacks. Full retrieval of data is not possible after attacks. On the other hand DWT is more robust to attacks.*

Keywords*: steganography, LSB, DWT, stego-image, discrete wavelet transform, least significant bit*

I. INTRODUCTION

The 21st century has brought with it the dawn of assailability. Whenever we communicate via a medium the security of our message becomes an inevitable concern. Steganography provides us with data hiding capabilities. Steganography can be viewed as kin of cryptography .No one apart from sender and recipient suspects the existence of the message in steganographic techniques. In this paper we are analysing LSB and DWT technique for data security applications [1]. LSB technique is the most basic spatial domain method in image steganography, where a message is embedded in the insignificant bits of a cover. On the contrary DWT is a frequency domain method where data is embedded by altering the frequency coefficients. Transform domain methods embed messages in significant area of cover image which makes them robust against various operations and attacks like cropping, rotation and image compression. Thus DWT provides a very secure way of communicating confidential data through an unsecure medium. Though LSB provides better embedding capacity but it is prone to even small cover modifications.

II. LSB TECHNIQUE

Least significant bit (LSB) [6] insertion is a common, simple approach to embedding information in a cover image. For instance, a simple scheme proposed, is to place the embedding data at the least significant bit (LSB) of each pixel in the cover image. The altered image is called stego-image. Altering LSB doesn't change the quality of image to human perception but this scheme is sensitive a variety of image processing attacks like compression, cropping etc [4].

- PROPOSED ALGORITHM

Embedding Algorithm:
Input: cover image, key, secret message
Procedure:
Step1: Take a gray scale image(8-bit).
Step2: Convert the secret message into bit stream.
Step3: Now generate the sequence of indices for bit insertion. Here odd bits of the stream is embedded in IJthlocation and the even bit is embedded in JIth location. We increase IJ by some stepsize and proceed respectively
Step4: While complete bit stream not embedded
Reduce the value of stepsize by some constant value and replace least significant bit of pixel at IJth location.
End.
Output: Stego-Image.
On the receiver side extraction of this secret message is performed. The receiver has the knowledge about the key and the length of the secret message.

Extraction Algorithm:
Input: stego-image, key
Procedure:
Step1: Take the stego-image
Step2: Calculate the pixel positions in the same way as in the embedding algorithm by using the same key.

Step3: Form the secret bit stream by the LSB's of these pixels.
Step4: Convert this bit stream into the corresponding ASCII value by using 8-bit conversion.
End
Output: Secret-Message

III. DISCRETE WAVELET TRANSFORM

A small wave is called a wavelet. A wavelet is a waveform of effectively limited duration that has an average value of zero .The term wavelet comes from the fact that they integrate to zero .Orthogonality is an important property, it ensures that a data is not over represented, it can be decomposed into various scaled and shifted version of the mother wavelet [1].
The wavelet transform is basically a multi –resolution decomposition process. DWT [5] gives an excellent space ,frequency localization. The input image is divided into 4 non over lapping sub bands LL,HL,LH,HH. The LL region has the most significant information .it provides large space for embedding data and is more robust .
Here we are using HAAR wavelet because it is not continuous , small changes in the input does not result in small changes in output and not differentiable. This wavelet was given by AlferdHaar.

- PROPOSED ALGORITHM

Embedding Algorithm:
Input: cover-image , secret message
Procedure:
Step1: Take the cover image and the secret message to be embedded.
Step2: Preform 8x8 blocking on the cover image.
Step3: Take the first block and perform third level of decomposition on it.
Step4: Convert the secret message into bit stream.
Step5: Embed the first bit of the bit stream in the LH3 level of the first block .
Step6: Repeat steps 3 and 5 on the consecutive blocks until all the data is embedded in the image.
End.
Output: Stego-Image.
Extraction Algorithm:
Input: Stego-Image
Procedure:
Step1: take the stego-image.
Step2: Preform 8x8 blocking on the stego-image.
Step3: Now perform inverse DWT on each block.
Step4: Extract the bits from the blocks to form a bit stream and convert them to the ASCII values.
End
Output: Secret-Message

IV. COMPARES AND ANALYSIS OF ALGORITHMS AGAINST SEVERAL ATTACKS

This paper compares and analysis least significant bit technique (LSB) and discrete wavelet technique (DWT) on the basis of several attacks like compression, cropping, rotation and contrast enhancement. These comparisons are being used to determine the robustness of the above mentioned techniques.

- **COMPRESSIO**

Compression is the process by which we reduce the redundancy of image data so that we can store and transmit data efficiently. Compression can be of 2types, lossy and lossless compression. If after compression we can recover every single bit of the data originally present in the file, then it is called lossless compression else it is known as lossy compression.

- **CROPPING**

Refers to the removal of the outer parts of an image to improve framing, accentuate subject matter or change aspect ratio. Depending on the application, this may be performed on a physical photograph, artwork or film footage, or achieved digitally using image editing software. The term is common to the film, broadcasting, photographic, graphic design and printing industries.

- **ROTATION**

The rotation operator performs a geometric transform which maps the position (x1,y1) of a picture element in an input image onto a position (x2,y2) in an output image by rotating it through a user-specified angle about an origin . Rotation is most commonly used to improve the visual appearance of an image.

- **CONTRAST ENHANCEMENT**

The word contrast refers to the difference in luminance or gray level value in an image. It can also be defined as the ratio of the maximum intensity to minimum intensity over an image. Contrast enhancement is a technique that expand the range of brightness values in an image so that image can be efficiently displayed in a manner desired by the analyst.

V. RESULT AND CONCLUSION

Table1: Retrieval Of Data After Performing Attacks On LSB and DWT

VARIOUS TECHNIQUES	COMPRESSION			CROPPING		ROTATION	CONTRAST ENHANCEMENT
	5%	10%	15%	10%	20%	CLOCKWISE 90°	
LSB	20%	15%	10%	15%	7%	25%	10%
DWT	70%	55%	50%	90%	75%	80%	70%

This table shows the comparison of LSB and DWT with various attacks. In LSB when we compressed the stego –image by 5%,only 20% of the embedded data is retrieved. On the other hand, in DWT, the percentage of data retrieved at 5% of compression is 70%, which is three times the data retrieved in LSB. The percentage of retrieved data decreases as the percentage of compression is gradually increased. When we crop,rotate and perform contrast enhancement on the stego –images in LSB as well as in DWT we conclude that the data retrieval is more in DWT as compared to LSB. From these results we conclude that LSB is more vulnerable to even small cover modifications than its counterpart. Hence DWT is more robust to attacks as compared to LSB.

REFERENCE

[1]. Ali Al-Ataby and Fawzi Al-Naima, “A Modified High Capacity Image Steganography Technique Based onWavelet Transform”, The International Arab Journal of Information Technology, Vol. 7, No. 4, October 2010.
[2]. Abbas Cheddad, Joan Condell, Kevin Curran and Paul McKevitt “Digital image steganography :survey and analysis of current methods’’. Signal processig, volume 90,March 2010,pages 727-752.
[3]. Hong-Juan Zhang, Hong-Jun Tang, "A Novel Image Steganography Algorithm Against Statistical Analysis", Proceedings of the Sixth International Conference on Machine. Learning and Cybernetics, Hong Kong, 19-22 August 2007.
[4]. Fahimirfanalam , Fatehakhanambappee , Fariduddinahmedkhondker “An investigation into encrypted message hiding through images using lsb” Vol. 3 No. 2 Feb 2011
[5]. TanmayBhattacharya ,NilanjanDey and S. R. BhadraChaudhuri:“Novel session based dual steganographic technique using dwt&spread sprectrum”: Vol.1, Issue1, pp-157-161.
[6]. Chan, C. K. and Cheng, L. M. 2003. Hiding data in image by simple LSB substitution. Pattern Recognition, 37:469-474.

